AMENDMENTS TO THE SPECIFICATION

Please amend the paragraph starting on page 1, line 16, as follows:

--In conventional cryptosystems, cryptographic~~crypotographic~~ algorithm is derived from mathematical models. It makes people believe it is impossible to extract secret key with a low complexity algorithm. However some problems caused during cryptographic~~crypotographic~~ implementations are not considered within mathematical models and what allows attacks to find out the secret keys via some indirect techniques such like microprobing, reverse engineering, memory read-out techniques, etc. To prevent these attacks, a variety of physical techniques for protecting cryptographic devices are known, including enclosing key management systems in physically durable enclosures, coating integrated circuits with special coatings that destroy the chip when removed, and wrapping devices with fine wires that detect tampering. However, these approaches are difficult to use in single-chip solutions (such as smartcards), and difficult to evaluate since there is no mathematical basis for their security. Physical tamper resistance techniques are also ineffective against some attacks.--

Please amend the paragraph starting on page 3, line 21, as follows:

--According to "Paul C. Kocher in his paper, Timing attacks on implementations of Diffie-Hellman, RSA, DSS, and other systems, Proceedings of Crypto '96, 1996", and "Paul C. Kocher in his paper, Kocher, Cryptanalysis of Diffie-Hellman, RSA, DSS, and other systems using timing attacks, Dec. 7, 1995", some information about the cryptographic~~crypotographic~~ key leak out by measuring the length of cryptographic computation.--

Please amend the paragraph starting on page 5, line 15, as follows:

--As the aforementioned, operation of modulo-multiplication or modulo-squaring occurs at any particular time is controlled by a conditional jump (line 4 in FIG.1) that depends on the value of the exponent, e, as it is traversed, commonly bit-by-bit. Based on this simple theory, there is an improved cryptographic~~crypotographic~~ algorithm which is shown in FIG.3. This algorithm reduces leakage from cryptosystems by implementing critical operations using fixed execution path routines whereby the execution path does not vary in any manner that can reveal useful information about the secret key during subsequent operations so as to protect cryptographic~~crypotographic~~ keys against timing attacks and power monitoring attacks.--

Please amend the paragraph starting on page 6, line 19, as follows:

--Fault attacks try to introduce errors into the cryptographic~~crypotographic~~ computation, and to identify the key by analyzing the mathematical and statistical properties of the erroneously computed results. Among the many techniques that suggested so far for introducing such errors are the uses of ionizing radiation, unusual operating temperatures, power and clock glitches, and laser-based chip microsurgery.--

Please amend the paragraph starting on page 7, line 1, as follows:

--C safe-error attacks introduce temporal error within ALU so as to induce temporal erroneous computation. Some of the attacks carry out an erroneous computation, while others won't. Upon these different outputs, some information of the cryptographic~~crypotographic~~ key will be revealed. In FIG.3, when some $e_k = 0$, $S_b = (S_b \bullet S_2) \bmod n$ is a redundant computation. It is to say that if a temporal error is introduced during this computation, it will induce an erroneous computation but this erroneous result will not affect the next computation cycle, so the final output will still be the same. If the attacker introduce a single error at a random time during the computation of $S_b = (S_b \bullet S_2) \bmod n$, by observing whether the output of the computation is with error or not, the attacker can realize the corresponding bit of the secret key. If the output is with error, the corresponding digit of the secret key is 1; otherwise, the corresponding digit of the secret key is 0.--

Please amend the paragraph starting at page 9, line 5, as follows:

--In accordance with the present invention, a novel cryptographic~~crypotographic~~ algorithm is provided that substantially overcomes the drawbacks of the above mentioned problems.--

Please amend the paragraph starting on page 9, line 14, as follows:

--It is another object for present invention to provide a modular exponentiation algorithm without any redundant calculation in it so as to be substantially immune from the~~both~~ C safe-error attack.--

Please amend the paragraph starting page 10, line 16, as follows:

--This invention provides a method, an apparatus or a computer-readable medium for protecting public key schemes from timing, power monitoring and fault attacks comprising the steps of: 1. obtaining a message for use in a cryptographic~~crypotographic~~ operation; 2. obtaining a modulus and an exponent corresponding to said cryptographic~~crypotographic~~ operation, wherein said exponent contains at least one bit; 3. initializing a first value as [[a]] one, and assigning the message to a second value; 4. executing a modulo exponentiation algorithm on each bit of the exponent from a most significant bit to a least significant bit, wherein the algorithm comprising the steps of: a. input a bit to an inverter and storing the output as a third value, and assigning the next bit of the exponent as a fourth value; b. if the third value is a zero, updating the first value with the result of squaring, modulo the modulus the first value, if the third value is [[a]] one, updating the first value with the result of multiplying, modulo the modulus said first value by the second value; and c. if the fourth value is [[a]] zero, updating the first value with the result of squaring, modulo the modulus the first value, if the fourth value is [[a]] one, updating the first value with the result of multiplying, modulo the modulus the first value by the second value; 5. updating the bit with the next bit of the exponent, and executing steps of the algorithm on the bit until the bit being the least significant bit of the exponent; and 6. storing and output the first value.--

Please add the following paragraph after the paragraph ending on page 11, line 15:

--Further scope of the applicability of the present invention will become apparent from the detailed description given hereinafter. However, it should be understood that the detailed description and specific examples, while indicating preferred embodiments of the invention, are given by way of illustration only, since various changes and modifications within the spirit and scope of the invention will become apparent to those skilled in the art from this detailed description.--

Please amend the paragraph beginning on page 11, line 19, as follows:

--The ~~foregoing aspects and many of the attendant advantages of this~~ present invention will become more ~~readily appreciated~~ fully ~~as the same becomes better~~ understood ~~by reference to~~ from the following detailed description~~, when taken in conjunction with~~ and the accompanying drawings, which are given by way of illustration only, and thus are not limitative of the present invention, and wherein:--

Please amend the paragraph starting at page 13, line 22, as follows:

--The present invention provides an algorithm as in FIG.4. At the beginning, obtaining a message M for use in a cryptographic~~crypotographic~~ operation and an exponent $e=(e_{w-1}, e_{w-2},\ldots, e_1, e_0)$ and a correlated modulus n then initializing $S_0=1$, assigning M to S_1, and let $e_{-1}=1$ (100), then set $k=w-1$ and executing a modulo exponentiation algorithm on each bit of the exponent from the most significant bit (e_{w-1}) to the least significant bit (e_0), wherein the algorithm comprising the steps of: **1.** Input the bit e_k to an inverter and storing the output as a value b, and assigning the next bit e_{k-1} as a value c; **2.** Executing $S_0=(S_0 \cdot S_b)$ mod n and $S_0=(S_0 \cdot S_c)$ mod n (130) **3.** Executing $k=k-1$ (140); **4.** Repeating step 1 to step 3 until finishing the loop of $k=0$; **5.** Storing and output S_0 (150).--